Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2004 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2004

Security, Privacy and a Trusted Information Intermediary: A Compensation Model and Markets for Private Information

Daniel Rice
Loyola College in Maryland

Robert Garfinkel
University of Connecticut

Ram Gopal
University of Connecticut

Security, Privacy and a Trusted Information Intermediary: A Compensation Model and Markets for Private Information

Daniel O. Rice
Loyola College in Maryland
drice2@loyola.edu

Robert S. Garfinkel
University of Connecticut
robert.garfinkel@business.uconn.edu

Ram D. Gopal
University of Connecticut
ram.gopal@business.uconn.edu

ABSTRACT

Technological advances in the collection, storage, and analysis of data have increased the ease that businesses can turn mounds of personal data into useful information. Economic value is being created through the analysis of personal data. Meanwhile, individuals are increasingly becoming aware of the value of their personal information. Privacy concerns further lead some individuals to guard their personal information from disclosure. This paper explores a market for personal information. This economic system requires a flexible approach to data protection because subjects are compensated based on the amount of disclosure of personal information. Compensation is linked through a data protection model based on Confidentiality via Camouflage (CVC) presented in Gopal et al. (2002). A trusted information intermediary (TII) ensures that security and other desired market conditions exist allowing for a self-regulated market. A working model and example flexible security and compensation is presented and analyzed using simulation.

Keywords

Privacy, data protection, information intermediary, electronic markets, information markets, information security

INTRODUCTION

The private information products discussed in this paper are information goods compiled from personal information of either individuals or establishments. Rose (1999) defines private information as "information that is produced privately and can be hidden." Transacting on private information necessitates careful consideration of privacy which is the "right of an individual, group, or institution to determine when, how and for what purpose information concerning himself/itself can be collected, stored and released to other people or entities" (Castana, Fugini, Martella, and Samarati 1995). Safeguarding privacy entails the ability of these entities to determine when, how and for what purpose their personal information is to be used.

Naturally, individuals tend to want to protect their personal information. However, individuals often are willing to provide personal information, if they think it will be put to good use and handled confidentially. For example, customers are often willing to complete surveys from a business they patronize and patients often provide personal information to doctors and medical research. Many businesses provide incentives to entice individuals to allow the organization to collect and use their private information (Laudon 2000). This incentive is often in the form of monetary compensation. However, an issue certainly as important as compensation is that of reassuring contributors of information that their private information will not fall into the wrong hands. This research presents a model of market intermediation between the users and owners of private information. We introduce a trusted information intermediary (TII) that performs the vital roles of compensation and protection in a market for private information.

A MARKET FOR PRIVATE INFORMATION

There are many possible realizations of a TII for a private information market. One such possibility is an idea presented in Laudon (1996), the National Information Marketplace (NIM). The NIM would have the ability to track individuals' private

information as well as the capability of providing compensation to contributors of private information when it is used. However, the NIM conjures up thoughts of a very large centralized database system that has control of an abundance of personal and private information. To many, this concept is very undesirable due to concerns that once the NIM is implemented it would be exposed to inherent risk of attack, and even worse, subject to abuse by the controllers of the information. Still, the business need for good private information is ever present. This demand coupled with an abundant supply of private information (information that is becoming easier to collect, store and analyze) lead us to predict that small independent TIIs will emerge everywhere to meet the specialized information needs of businesses. We investigate the role of the TII in a market for private information, especially where it relates to incentives and security.

RELATED RESEARCH – PRICING INFORMATION IN ONLINE SERVERS

The problem of pricing information has been studied from several different angles in the information systems literature. The problem of pricing the access to information servers includes server connect time strategies (Gupta, Stahl, and Whinston. 1997), pricing mechanisms solved as resource allocation problem and from a quality of service perspective (Gupta et al. 1999), access pricing of information, that is modeled as a public good and based on a combination of per record search and connect time strategy (West 2000) and the pricing of access based on a successful search. (Jain and Kannan 2002). All of these models take into account the use of resources and the cost of processing queries, as well as the value of the information in query answers. However, none have addressed the security of confidential data in the context of answering queries. In this paper, we explicitly model the trade-off between the value of information given in a query answer to a consumer and the security of the private information used in answering the query. Economic analysis of this trade-off is used to investigate information pricing, subject compensation, and other market considerations.

The emergence of electronic markets and market intermediaries who serve those markets have recently gained some attention in information systems literature. More specifically, recently substantial interest has been shown in the economics of information intermediaries and their emerging roles in electronic commerce. Some recent studies that focus on the economics of intermediaries contributes value added services such as product aggregation and networking buyers and sellers, pricing strategies of the information intermediary, and quality of service. (Corbett and Karmarkar 1999, Bhargava and Choudhary 2003, Bargava, Choudhary, and Krishnan 2003). These studies are closely related to the study of an intermediated market of private information; however, they tend to focus on the information intermediaries who connect buyers and sellers for physical products where the TII is a pure information intermediary who serves as information buyer, processor and vendor. Still, our information intermediary can takes advantage of some of the same benefits discussed in these earlier papers such as that of adding value to the information and providing the incentive that allows for linking of sellers and buyers in the market.

A MARKET FOR PRIVATE INFORMATION

There are many possible realizations of a TII for a private information market. One such possibility is an idea presented in Laudon (1996), the National Information Marketplace (NIM). The NIM would have the ability to track individuals' private information as well as the capability of providing compensation to contributors of private information when it is used. However, the NIM conjures up thoughts of a very large centralized database system that has control of an abundance of personal and private information. To many, this concept is very undesirable due to concerns that once the NIM is implemented it would be exposed to inherent risk of attack, and even worse, subject to abuse by the controllers of the information. Still, the business need for good private information is ever present. This demand coupled with an abundant supply of private information (information that is becoming easier to collect, store and analyze) lead us to predict that small independent TIIs will emerge everywhere to meet the specialized information needs of businesses. We investigate the role of the TII in a market for private information, especially where it relates to incentives and security

THE TRUSTED INFORMATION INTERMEDIARY

There are many real life examples of existing TIIs. One such example is the US Census Bureau. The Census Bureau elicits private data from individual citizens, stores the data, conducts analysis and disseminates information based on the private data, usually in the form of meta-data, to parties who derive economic value from that information. Most individuals are willing to provide accurate information to the census bureau because the information is put to a good use and their privacy is protected. The Census Bureau's goal is "to provide the best mix of timeliness, relevancy, quality, and cost for the data we collect", and their mission includes a commitment to "honor privacy" and to "protect confidentiality" (www.census.gov).

We can view firms as intermediation mechanisms whose task is to select feasible input-output plans and to make production decisions, such as deciding what technology to adopt, given market prices. The firm as intermediary keeps track of production accounts, inputs and outputs, and profit accounts, costs and revenues and must decide whether or not to enter output markets based on their knowledge of production and profit accounts. The intermediary also makes technology decisions based on these accounts (Spulber 1999). Trust becomes critical for a market for private information and trust is critically linked to both sides of the production function. Users must trust that the TII is giving good and fairly priced information and the subjects must trust that private information is protected. Therefore, a TII serves two essential trust related functions in a market for private information: they provide incentive for participation in the market; and, they protect against the misuse of private information.

ECONOMIC FOUNDATIONS

A market for private information requires that we explicitly address and incorporate the security dimension into the market model. A supply of private information will be available only if individuals are willing to contribute. Incentive to contribute private information may come from various motivations including the providing of a benefit to mankind, economic compensation, or even increasing customer's expectation of better service in the future. Regardless of the source of the motivation, potential contributors must be reassured that their private information is protected from falling into the wrong hands. Demand exists when there are information consumers who desire access to private information. One such reason for a "desire" to access to private data is potential for economic gain. We concentrate our analysis on "legitimate" information users. That is, a user who uses private information to gain business intelligence rather than "snoopers" or "hackers" who may have other motives for accessing private information.

Therefore, our focus is on information consumers who intend to use information in business analysis and want to create economic value through access to private information. There may be hundreds of thousands of companies worldwide who exemplify this type of demand. Usually, the demand is given names such as Customer Relationship Management (CRM) or data-mining, where useful information is mined from mounds of private data. Stating that we are less interested users who are trying to hack into, attack or steal private information doesn't mean that we can ignore the potential for this type of undesirable demand. In fact, we must protect against it. We realize the importance of this issue. However, the central focus of this paper is the design and implementation of the market for private information and we ignore what could be considered "hostile" demand.

On the other hand, we are very interested in companies who would like to access private information in order to perform some sort of aggregate analysis using the private information and gearing the analysis to understanding particular groups of people. Marketing information exemplifies this type of demand, where individuals' private data is use for demographic analysis, data-mining and CRM. Still, we envision many other potential consumers in the market for private information including government organizations, health care, universities and a wide variety of other public and private organizations.

We've seen that the economic desiderata for this private information market are rather intuitive. Supply - individuals must have incentive to contribute private information and they must and be assured that the information will be protected. Demand - information consumers must find real economic value in the information served implying that the information should at least be "good" information. Naturally, the entire system should be protected with other levels of security that is adequate to protect against hacking, spoofing, intercepting or and inference leak. Each of these could lead to the unwanted disclosure of private information. We require adequate protection on the physical, software, operating system, networking, and internetworking levels and we assume that this is achievable (or, as achievable as it is on any other online database system).

The security discussion in this paper closely addresses the threat of inference. This involves the market imperative that information consumers should only be able to get the information they have bought. That is, they should not be able to infer any additional information from the information they consume. This last point is subtle but critical. In a market where there is incentive to cheat, a private good may quickly be transformed into a publicly available good, and the market subsequently collapses. In other words, a market for private information is not sustainable when there is a high likelihood that private information is spuriously released either directly or indirectly through inference channels. It is clear that market for private information is inextricably linked to the security mechanism. That is, you cannot have a market for private information without the security in place that will protect the confidentiality of that information.

The market for private information is modeled as an interaction between three players: (1) the DB subjects who contribute private information; (2) the TII; and (3) DB users. The inclusion of the subjects in the market is noteworthy as it

differentiates this research from other research models found in economic analysis of online databases vendors. Moreover, it indicates that DB subjects will require compensation for the use of their private information. This reflects a recent trend that individuals are becoming more and more aware of the value of their personal information and in the future individuals will become less and less willing to just "give away" valuable information. Our model gives the DB subjects an increased role in the market. This increased role is seen in many real life examples where individuals are requiring fair compensation for the use of their personal information (Laudon 1996). In this paper, we explicitly model the role of the contributors of private information.

SECURITY

The protection of private data is critical in a market for private information. Inability to protect private data may lead to market failure; not to mention that subjects will be unwilling to contribute private information if they feel that it may fall into the wrong hands. The role of TII is double-headed. First, the TII must provide good information to paying customers who query the database. Second, the TII must secure private information stored in the database. The model presented in this paper provides a mechanism that allows the TII to vary the quality of answers, (that is, allows the TII to give "better" or more exact query answers if the DB user is willing to pay for better answers). Better answers generally imply a decrease of privacy protection of DB subjects who have an agreement with the TII that allows the TII to decrease protection if DB subjects are appropriately compensated.

Data confidentiality models that address the protection sensitive numerical information stored in databases include perturbation, query restriction, and CVC (data-hiding) techniques. Perturbation refers to database security as the changing of numerical data systematically so that a user querying the data cannot determine confidential data with any certainty. Query restriction, on the other hand, refers to restricting access to data when access potentially leads to disclosure of confidential fields of data. Data-hiding techniques allow for answering queries, but, camouflaging the actual data so that it cannot be derived from the answers. The Confidentiality via Camouflage (CVC) approach to data security is unique in that it incorporates the advantages of both perturbation and query restriction while eliminating some of the major disadvantages. (Gopal et al. 2002). The CVC approach allows deterministically correct answers in the form of an interval that corresponds to a point answer. There is a deterministic guarantee as to the maximum deviation from the exact correct answer. The answer is an interval and the protection is noted as "interval protection". Gopal et al. (2002) demonstrates the use of CVC in the protection of confidential numerical information. While each of the above confidentiality methods has advantages and disadvantages, for the purpose of protecting private data in a market environment as described in this paper we use a version of CVC called CVC-STAR.

CVC-STAR provides a protection foundation that the economic mechanism is built upon. CVC-STAR has some very promising characteristics, including protection against insider inference threat, as well as providing an underlying protection instrument that fits well with the adjustable protection, varying the quality of answers, and the economic concepts crucial to this research. Details of CVC-STAR are found in Garfinkel, Gopal and Rice. (2004).

BOUND PROTECTION

Bound protection allows a DBA to answer queries using private numerical data by creating a protection interval. The interval is formed from a lower protection bound and an upper protection bound and it the private data point falls between the protection interval bounds. Answers to queries using the private data are calculated based using the bounds. The upper and lower bounds of the answer interval are found by answering the query using the protection bounds, or some combination of the protection bounds and the actual data (as in CVC-STAR). Answer intervals are guaranteed to be deterministically correct. That is, the answer interval is guaranteed to contain the actual answer. We use the concepts of bound protection and answer intervals to develop a security model that fits into our investigation of a market mechanism that will protect the privacy of individual subjects and meet the information needs of database users.

A protection interval is a measurement of the distance between the upper and lower protection bounds. Consider the example database below. This database table contains N=3 records, “salary” is the private attribute; P^L and P^U are protection vectors that exist to protect the private information. Every subject *s* is afforded a protection interval $\Gamma_s = \left[p_s^{\ell}, p_s^{u}\right]$ and a range of protection $\gamma_s = \left[p_s^{u} - p_s^{\ell}\right]$. For example, Smith’s protection is Γ_1 = [45, 100] and the range is γ_2 = 55. The database is protected by the set of protection intervals, $\mathbf{\Gamma}$ = [Γ_1,…, Γ_N].

Subject	Name	Occupation	Salary	P^L	P^U
1	Brown	Engineer	75	50	90
2	Smith	Engineer	55	45	100
3	Jones	Teacher	45	40	80

Table 1 – Example Database Relation

ANSWER QUALITY

The quality of an answer interval is defined by comparing the answer interval to a known answer interval that includes all feasible answers termed as the "known interval". This definition is reasonable if we assume that for any query asked, there exists an upper bound and a lower bound of that answer. The user's knowledge of bounds is assumed because "it is common to release upper and lower bounds for data without identifying the specific records." (Pfleeger and Pfleeger 2003). Even in the case that the TII does not release known bound information, it is reasonable to assume a user could assign meaningful bounds for query answers. We assume that the TII provides bound information and provides the user with a quality measurement, k. Computing quality level k is a simple calculation that compares the answer interval range to the known interval range. For example, consider a query that asked Smith's salary. Perhaps it is known that no engineer in the database has a salary lower than 35 or higher that 135. Then, the quality of the answer would be calculated as $k = 1 - \frac{(100-45)}{(135-35)} = 1 - \frac{55}{100} = 0.45$. The measurement of quality is important, especially when we consider improvements to quality through the reduction of protection intervals.

A COMPENSATION MODEL FOR A PRIVATE INFORMATION MARKET

The market for private information involves three key players: (1) DB subjects (2) the TII; and (3) DB users. Two pricing cases are analyzed; fixed-rate pricing (no shrinking) and variable-rate pricing (shrinking) where the quality of query answers are tailored to meet users' quality specifications. Customizing the answer quality may require the TII reduce individuals' privacy protection for each query answered. Subjects are afforded an original protection interval and shrinking of a subjects' protection interval varies from zero (no shrinkage, full protection) to one (total shrinkage, no protection). We assume that after each user query the DB reverts back to its original state.

Fixed-rate Pricing

A DB user i is charged a fixed-rate price, p_f, for each record accesses when answering user i's query. The user derives benefit $B_i[t_i]$ that is a function of the query cardinality t_i and the user's utility is:

$$\Pi_i = B_i[t_i] - p_f * t_i$$

The TII will share profits (sharing multiplier $\alpha \in [0,1]$) with each subject when a subject's record is used in answering a query giving the following utility functions for the TII and for each subject s, respectively:

$$\Pi_{TII} = \alpha \sum_i \left(p_f * t_i \right)$$

$$\Pi_s = (1-\alpha) \sum_i \left(x_i * p_f \right)$$

where $x_i = 1$ if subject s is included in a query by user i, $x_i = 0$ otherwise.

Variable-Rate Pricing

In the case of variable-rate pricing the users' benefit increases with higher quality answers. Quality of answers can be improved by the manipulation of protection bounds. We assume that benefit is non-decreasing in query cardinality and quality. That is, as query cardinality increases, or quality increases, the benefit to the user will either increase or stay the same. Every subject *s* is afforded a protection interval $\Gamma_s = \left[p_s^{\ell}, p_s^{u}\right]$ and a range of protection $\gamma_s = \left[p_s^{u} - p_s^{\ell}\right]$. The, the database with a total of N records is protected by the set of protection intervals, $\mathbf{\Gamma} = [\ \Gamma_1,\ldots,\ \Gamma_N\ ]$. When a protection interval is reduced, we define the reduction by the ratio of the new protection interval range to the original protection interval range. For a query by user *i*, the reduction in protection for the database is defined by the set $\Theta_i = \left[\theta_1,\ldots,\theta_{t_i}\right]$ where the reduction of protection for subject *s* is denoted θ_s where $\theta_s = 1 - \left(\frac{\gamma'_s}{\gamma_s}\right)$. ($\theta_s \in [0,1]$ for all *s* where $\gamma_s \geq \gamma'_s$, otherwise $\theta_s = 0$).

User *i*'s utility function is:

$$\Pi_i = B_i\left[t_i, k\left(\Theta_i\right)\right] - p_f * t_i - \sum_{s=1}^{t_i} p_s * \theta_s$$

Note that the 3rd term in the utility function reflects the charge for the reduction in protection bounds in answering user i's query. It follows that the TII charges for answering queries and subjects are compensated given by the following profit functions:

$$\Pi_{TII} = \alpha\left(\sum_i \left(p_f * t_i\right) + \sum_i \sum_{s=1}^{t_i} p_s * \theta_s\right)$$

$$\Pi_s = (1-\alpha)\left(\sum_i \left(x_i * p_f\right) + \sum_{s=1}^{t_i}\left(p_s * \theta_s\right)\right)$$

AN EXAMPLE PROBLEM

For the example problem and simulation we assume a user benefit function that is increasing in cardinality and in quality, so that user i's utility function is:

$$\Pi_i = C * \left(t_i\right)^{\frac{1}{2}(1+k)} - p_f * t_i - \sum_{s=1}^{t_i} p_s * \theta_s$$

where $C = 15$, $p_f = 1$ and $p_s = 1$.

The details of calculating answers using CVC-STAR and shrinking protection intervals are not included into this paper so that we may concentrate on the economic issues of the work. For the purpose of the examples and simulation, the reader should note that CVC-STAR is used to calculate answer intervals as they are shown here. For a more detailed discussion of CVC please refer to Gopal et al. (2002).

For this example consider two users, each who ask one query to the example database (Table 1 above).

Query 1 - user 1 asks query Q_1: "What is the sum of the salaries of Engineers?"

The selected record set is T = {1,2} and the query cardinality is $t_1 = 2$. Using CVC-STAR, the query answer is given as I_1 = [105,175] and $k_1 = 0.65$. User profit is calculated and rounded to two decimal places as $\Pi_{i=1} = 24.57$. The profit of the TII is calculated to be $\Pi_{TII} = 1$ and profits of the two subjects is calculated as $\Pi_{s=1} = 0.5$ and $\Pi_{s=2} = 0.5$ (assuming they TII shares profits with subjects, that is $\alpha = 0.5$).

Query 2 - user 2 asks query Q_2: "What is the sum of the salaries of Engineers with $k = 0.70$?"

The selected record set an cardinality are the same as query 1, however the answer given is a tighter answer interval reflecting the quality constraint I_2 = [105,165] and $k_2 = 0.70$. Note that the reduction in the answer interval was achieved by

reducing subject 2's protection interval upper bound from 100 to 90, to give a new protection interval of $\Gamma'_2 = [45,90]$ and a new protection range of $\gamma'_2 = 45$. User profit increases because of the increase in benefit from a better quality answer and is calculated as $\Pi_{i=2} = 24.85$. The profit of the TII is calculated to be $\Pi_{TII} = 1.09$ and profits of the two subjects are calculated as $\Pi_{s=1} = 0.5$ and $\Pi_{s=2} = 0.59$.

Note from the example problem that User 2's profit is greater than that of User 1 which reflects User 2's additional utility due to a smaller answer interval. Also note that the TII and Subject 2 both enjoy a greater profit from query 2 if User 2 is willing to pay more for the higher quality answer. In the case of query 2, the User 2, the TII, and subject 2 all experience greater utility than in the case of query 1. This is an important observation because in clearly shows a case where there is incentive for market participation by all three players. Of course, user utility varies from user to user and is highly dependent on the TII's choice of query pricing. These issues are addressed in the simulation where DB users have varying levels of utility and the TII tries several different variable-rate pricing levels.

SIMULATION AND RESULTS

Simulation becomes necessary to verify the model because of the added complexities introduced by the use of the CVC-STAR algorithm, the shrinking of protection intervals, and overall dependence on the underlying data. The simulation verifies the model and explores the systems sensitivity to the costs (prices) associated with protection reduction.

We limit the simulation to SUM queries with a query cardinality of 100 because it allows the analysis to focus on the interaction between query quality, privacy protection, and compensation. However, simulation of other query types and the varying of query size are both possible extensions to the simulation analysis. It should be noted that this relatively simple simulation allows us to accomplish our objectives (1) capture demand from a group of users who have a value for query answers that is drawn from a normal distribution (2) capture the interaction between quality, shrinking protection bounds, compensation, pricing and the DB users' utility. We test 4 variable rate price scenarios $p_s = 0.25$, $p_s = 1$, $p_s = 2$, and $p_s = 3$.

The simulation scenario basically follows this sequence of events; the DB user submits a SUM query to a database, the user requests a query answer quality level, the TII answers the query by adjusting protection bounds where necessary to meet the requested quality requests, the TII then calculates the cost of the query, and finally the user decides to purchase the query if their value for answer is greater than price of the query answer.

The simulation models DB users arriving to ask queries, each who has a particular value and desired quality for a SUM query (each user's value is drawn as a normally distributed random variable with a mean of 400 and standard deviation of 100. Desired quality level is a value drawn as a uniformly distributed random variable where a user's required quality level k_i is varies between 0 and 1, that is $k_i \in [0,1]$. When a user asks a query with a desired quality level the TII finds the answer to the query and the cost, the user then will purchase if their overall utility is positive. The database used for the simulation contains 100 records. The following numbered steps further describe the simulation.

1. Query answer is calculated and compared to user specified quality level, if it meets or exceeds the specified quality level the simulation moves to step 3, calculating the DB user's utility for that particular query.
2. Subject protection bounds are reduced until the specified quality level is met.
3. DB user's utility is calculated
4. If the user's utility is positive, the query is purchased and profit calculated (step 5). If utility is zero or negative, there is no purchase and all profits for the query are zero.
5. DB user's profit is calculated (TII and subjects' profit also calculated). Otherwise, the query is not purchased and all profits are zero.

The experiment simulates 10,000 DB Users. There are approximately 250 observations at each quality level tested.

In addition to demonstrating the link between security and privacy in the simulation, an important result is learned that a TII should take note of when it comes to setting prices. How the TII sets prices for queries, specifically the variable-rate price p_s, has a significant impact on his profit and the profit of the subjects (remember, subject profit is incentive for participation in the market). First, if the shrinkage cost is set too high ($p_s = 2$ and $p_s = 3$) , the DB user will purchase less of the "high" quality queries and will settle for lower quality queries impacting both the TII's total profit and the total amount that DB subjects are compensated. On the other hand, if the price is set too low ($p_s = 0.25$) then DB users will purchase more queries and also

queries of higher quality. However, the trade-off is that the total TII profit and amount that subjects are compensated falls off dramatically as there is less revenue generated by answering high quality than in the case of higher p_s prices.

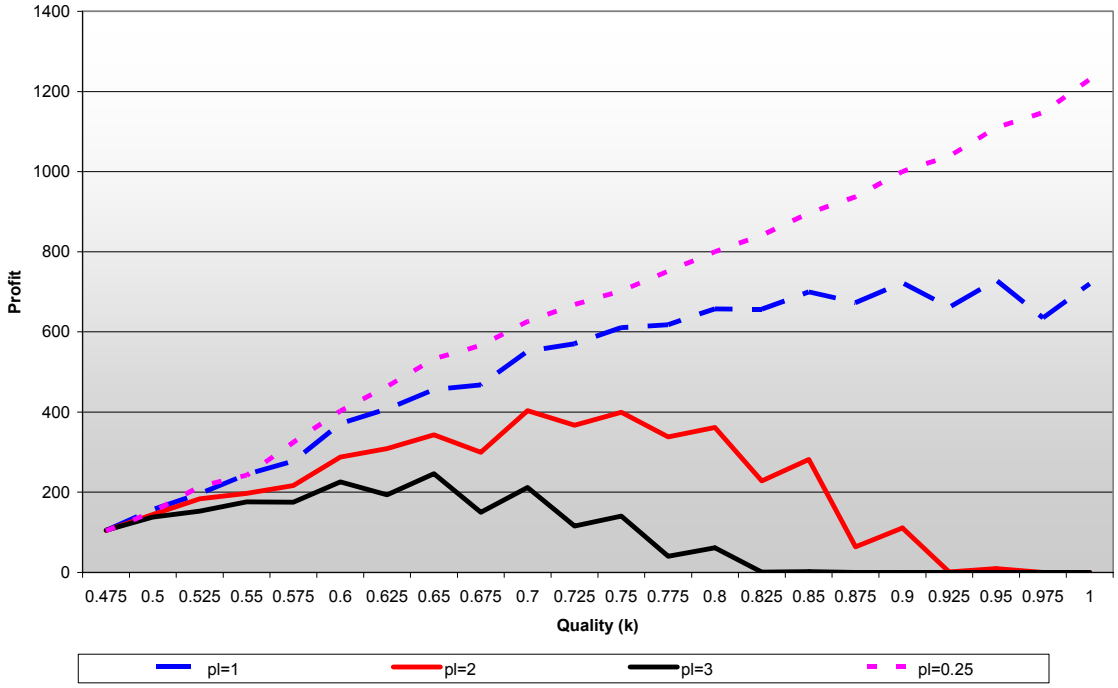

Figure 1. Average Profit of DB Users

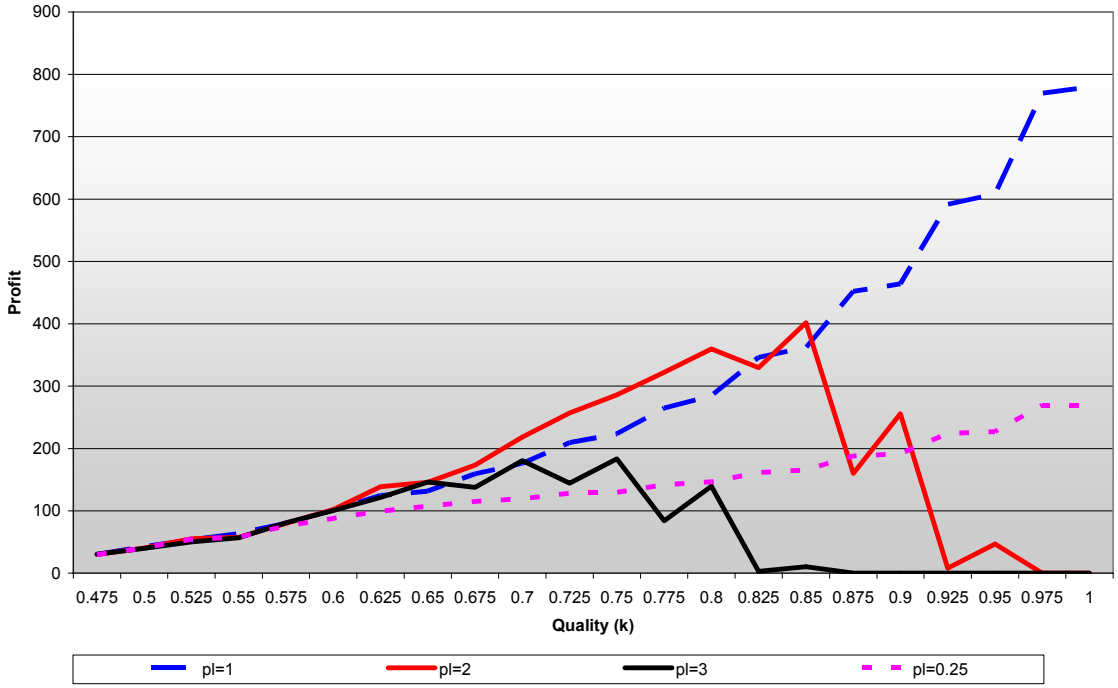

Figure 2. Average Profit of TII and Subjects

CONCLUSIONS AND FUTURE RESEARCH

We have introduced an economic model of the intermediation of an electronic market for private information. We have outlined the economic desiderata for a viable market, including the intermediaries role in providing incentive for participation by giving customize query answers and compensating DB subjects, as well as providing the necessary security that ensures market conditions are maintained and that the information contributors will be protected and private information will not be released without appropriate compensation. There are several important insights gained by modeling the market including how the market can be linked to and implemented with a security mechanism such as CVC-STAR to protect privacy. Additional insights pertain to decisions facing the intermediary such as pricing and compensation issues.

Although the research here is introductory in nature, it should be clear that the implementation of such a market is feasible using any standard database management system such as Oracle or SQL Server. Clearly, there is an abundance of future research work in this area that will lead to greater control of private information through incentive compatible economic mechanisms. First and foremost is the extension of the model to include all common query types. This will contribute to the practical implementation of a system that facilitates an intermediated market for private information. Furthermore, future research should investigate the creation of mechanisms that are capable of handling various data types including categorical and other non-numerical data.

The research presented here is exploratory in nature, and it is the authors hope that future research will strive to improve the links made between technical security research and the economic research. While very limited in scope, this study clearly shows that linking the two is feasible and valuable. The future of this research depends on security researchers who take into account the economic links with their work and design mechanisms that better fit into economic models of privacy. Likewise, economic researchers should strive to create economic models that are capable of incorporation security issues. Work to this end will not only prove valuable for research the area of a market for private information, but, will impact all areas of research in economics of information systems and security. There is certainly an economic balance that must achieved in every security question, such as the protection of privacy in the information age, it is up as information systems and economics researchers to search for that balance through continued work in this area.

REFERENCES

1. Bhargava, H., Choudhary, V., and Krishnan, R., Pricing and product design: intermediary strategies in an electronic market, working paper, Carnegie Mellon University
2. Bhargava, H. and Choudhary, V. (2003) Economics of an information intermediary with aggregation benefits, working paper, Carnegie Mellon University
3. Castana, S., Fugini, G.F., Martella, G., Samarati, P., Database Security, ACM Press published by Addison Wesley Longman Limited, England (1995)
4. Corbett, C. and Karmarkar, U. (1999) Optimal pricing strategies for an information intermediary, working paper, The Anderson School at UCLA
5. Chang, A.;Kannan P.K., and Whinston, A. (Fall 1999) The economics of freebies in exchange for consumer information on the Internet: an exploratory study, *International Journal of Electronic Commerce*, 4, 1
6. Garfinkel, R.; Gopal, R., and Rice, D. (2004) New approaches to disclosure limitation while answering queries to a database: protecting numerical confidential data against insider threat based on data or algorithms, working paper at The University of Connecticut
7. Gopal, R.; Goes, P., and Garfinkel, R. (May-June 2002) Confidentiality via camouflage: the CVC approach to database security. *Operations Research*, 50, 3
8. Gupta, A.; Stahl, D., and Whinston, A. (May 1997) A stochastic equilibrium model of Internet pricing, *Journal of Economic Dynamics & Control*, 21, 4,5 697-722
9. Gupta, A.; Stahl, D., and Whinston, A. (September 1999) The economics of network management, *Communications of the ACM*, 42, 9, 57-63
10. Jain S. and Kannan P.K, (September 2002) Pricing of information products on online servers: issues, models, and analysis. *Management Science*, 48, 9, 1123-1142
11. Laudon, K. (September 1996) Markets and privacy, *Communications of the ACM*, 39, 9, 92-104
12. Pfleeger, C.; Pfleeger, S. and Ware, W. (2002) Security in Computing 3e. New York: Prentice Hall
13. Rose, F. (1999) The Economics, Concept, and Design of Information Intermediaries: A Theoretic Approach, Physica-Verlag Heidelberg, Germany
14. Spulber, D. (1999) Market Microstructure: Intermediaries and the Theory of the Firm. Cambridge: Cambridge University Press
15. U.S. Census Bureau, About Us, http://www.census.gov/main/www/aboutus.html, Accessed on February 9, 2004
16. West, L. (Summer 2000) Private markets for public goods: pricing strategies of online database vendors. *Journal of Management Information Systems*, 17, 1, 59-86.